```
Set     Items   Description
S1     384156   WIRELESS OR WIFI OR WAP OR CELLULAR? OR MOBILE
S2       4323   (SECRET? OR PRIVATE? OR HIDDEN? OR CONCEAL?)(N)(KEY OR KEY-
                S)
S3        400   (CHANNEL? OR SELF()DISTRIBUTED)(N)(KEY OR KEYS)
S4     500519   STATION? OR PDA OR PORTABLE()DIGITAL()ASSISTANT? OR CELLPH-
                ONE? OR (CELL OR CELLULAR OR MOBILE)()(TELEPHONE? OR DEVICE? -
                OR LAPTOP? OR NOTEBOOK)
S5     898517   AUTHENTIC? OR VERIF? OR SECUR? OR ENCRYPT? OR ENCIPHER? OR
                ENCYPHER? OR CRYPTOG? OR PRIVACY OR PASSWORD? OR ID OR HANDSH-
                AKE? OR CRAM OR USER()(NAME? OR IDENTIFIER?)
S6           0   S1 AND S2 AND S3
S7         174   S1 AND (S2 OR S3) AND S4
S8     231390   ACCESS()POINT? OR BEACON? OR SERVER? OR BASE()STATION?
S9          87   S7 AND S8
S10         76   S9 AND S5
S11         24   S10 NOT AD=20000912:20030912
S12         20   S11 NOT AD=20030912:20050901
S13      73338   (CREATE? OR ESTABLISH? OR OPEN? OR GENERAT?)(2N)( ROUTE? OR
                 CHANNEL? OR PATH? OR CONNECTION?)
S14          5   S13 AND S7
S15          2   S2 AND S3 AND S13
S16          7   (S14 OR S15) NOT S12
File 347:JAPIO Nov 1976-2005/Apr(Updated 050801)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200552
         (c) 2005  Thomson Derwent
```

12/5/5 (Item 5 from file: 347)
DIALOG(R)File 347:JAPIO

05881562 **Image available**
METHOD AND SYSTEM FOR DELIVERING **SECRET KEY**

PUB. NO.: 10-164662 [JP 10164662 A]
PUBLISHED: June 19, 1998 (19980619)
INVENTOR(s): SHIGETAKE HIDEKI
APPLICANT(s): SHARP CORP [000504] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-320564 [JP 96320564]
FILED: November 29, 1996 (19961129)
INTL CLASS: [6] H04Q-007/38; H04L-009/08
JAPIO CLASS: 44.2 (COMMUNICATION -- Transmission Systems); 44.3 (COMMUNICATION -- Telegraphy); 44.4 (COMMUNICATION -- Telephone)

ABSTRACT

PROBLEM TO BE SOLVED: To provide a method and a system for delivering a **secret key** by which a fist **secret key** can be delivered even in a radio section between a **mobile station** and a public **base station** without using such a high-degree cipher system as the public key cryptosystem.

SOLUTION: After a **mobile station** (a) establishes an **enciphered** communication channel between the **station** (a) and a master machine A in which the **station** (a) is registered by using a preset second **secret key** KAa shared between the **station** (a) and machine (A), the **mobile station** (a) delivers a first **secret key** Kab to the machine A through the **enciphered** communication channel. Then the machine A delivers the first **secret key** Kab to a called wired terminal (b) through an ISDN 1.

12/5/6 (Item 6 from file: 347)
DIALOG(R)File 347:JAPIO

04335993 **Image available**
AUTHENTICATION METHOD IN DIGITAL **MOBILE** COMMUNICATION

PUB. NO.: 05-327693 [JP 5327693 A]
PUBLISHED: December 10, 1993 (19931210)
INVENTOR(s): KAMIBAYASHI SHINJI
KOBAYASHI KATSUMI
ONOE SEIZO
HANAOKA MITSUAKI
NAKAMURA HIROSHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
N T T IDOU TSUUSHINMOU KK [000000] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 02-402926 [JP 90402926]
FILED: December 17, 1990 (19901217)
INTL CLASS: [5] H04L-009/06; H04L-009/14; H04B-007/26
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 26.2 (TRANSPORTATION -- Motor Vehicles); 44.2 (COMMUNICATION -- Transmission Systems)
JOURNAL: Section: E, Section No. 1522, Vol. 18, No. 148, Pg. 132, March 11, 1994 (19940311)

ABSTRACT

PURPOSE: To enable a **mobile station** to be shared and to prevent illegal use by specifying a **authentication** confirmation signal and a **authentication** reply signal of a **mobile** set and a subscriber with a random number and a **secret key** and starting the operation when both the signals are coincident.

CONSTITUTION: A random number generating circuit 31 generates at first a random number R for an **authentication** request in a **base station** and transmits the number to a **mobile station** . A **mobile** set 30 enters the random number R and **secret keys** K(sub s), K(sub p) of the **mobile** set and subscriber to a signal conversion circuit 33 to obtain an **authentication** reply and a communication ciphering key K(sub e1) and transmits the **authentication** reply to the **base station** . The **base station** inputs the random number R and **secret keys** Ks, Kp to a signal conversion circuit 32 to obtain an **authentication** reply and a communication ciphering key K(sub e2). A comparator circuit 34 compares a bit pattern of the **authentication** reply received from the **mobile station** with a bit pattern of the **authentication** reply generated in the **base station** , and enables the **authentication** of the **mobile** set when they are coincident and disables the recognition in other cases. That is, then the **authentication** of the **mobile** set and the subscriber **authentication** are implemented simultaneously by one **authentication** procedure to share the **mobile station** by plural subscribers without degradation in the throughput.

12/5/12 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013594411 **Image available**
WPI Acc No: 2001-078618/200109
XRPX Acc No: N01-201123
Secure **transaction method for use between** mobile **terminal and** server **, involves establishing USSD dialogue between terminal and proxy till** secure **transaction is established**
Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF)
Inventor: KIESSLING J; VAN DO T; VAN THANH D; DO T V
Number of Countries: 094 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
NO 9902839	A	20001211	NO 992839	A	19990610	200109 B
WO 200078070	A1	20001221	WO 2000SE1169	A	20000606	200130
AU 200060312	A	20010102	AU 200060312	A	20000606	200121
NO 311000	B1	20010924	NO 992839	A	19990610	200159
EP 1186183	A1	20020313	EP 2000946576	A	20000606	200225
			WO 2000SE1169	A	20000606	
JP 2003502759	W	20030121	WO 2000SE1169	A	20000606	200308
			JP 2001504195	A	20000606	
US 6795924	B1	20040921	US 2000589810	A	20000609	200462

Priority Applications (No Type Date): NO 992839 A 19990610
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
NO 9902839	A			H04M-001/66	
WO 200078070	A1	E	16	H04Q-007/22	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW				
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW					
AU 200060312	A			H04Q-007/22	Based on patent WO 200078070
NO 311000	B1			H04M-001/66	Previous Publ. patent NO 9902839
EP 1186183	A1	E		H04Q-007/22	Based on patent WO 200078070
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
JP 2003502759	W		15	G06F-015/00	Based on patent WO 200078070
US 6795924	B1			H04L-009/00	

Abstract (Basic): WO 200078070 A1

NOVELTY - Proxy decomposes WML page from **WAP server** into USSD and sends data to **mobile** terminal display. After establishment of **secure** transaction, USSD dialogue is stopped and SAT application is activated in terminal. Application shows details of transaction and prompts for OK' to transaction. When user agrees, application signs data with **secret key** and sends to proxy where data is assembled in the WML format.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for **secure** transaction apparatus for use between **server** and **mobile** terminal.

USE - For enabling **secure** transaction between **server** and **mobile telephones** .

ADVANTAGE - Very high level of **security** is maintained due to the **security** aspect of the SIM card. The method can be used in different applications, as it got to handle only the signing process in SIM card. Information browsing and **security** of transaction are independent due to the system handling.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of **secured WAP** exchange using SAT back channel.

pp; 16 DwgNo 2/2

Title Terms: **SECURE** ; TRANSACTION; METHOD; **MOBILE** ; TERMINAL; SERVE;

12/5/15 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013153256 **Image available**
WPI Acc No: 2000-325128/200028
XRPX Acc No: N00-244799
Mobile **-communication dynamic** secure **grouping communication procedure, involves performing** encryption **communication between** base - station **and terminal using** base - station **group key**
Patent Assignee: KODO IDO TSUSHIN SECURITY GIJUTSU KENKYU (KODO-N)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2000101566	A	20000407	JP 98285872	A	1998092	200028	B

Priority Applications (No Type Date): JP 98285872 A 19980924
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000101566	A		12	H04L-009/14	

Abstract (Basic): JP 2000101566 A
NOVELTY - Two sets of disclosure key and **secret key** of intrinsic disclosure key system are selected and grouped as lot and are delivered to each terminal (2) forming terminal group key. The remaining disclosure key and **secret key** are formed as **base - station** group key and are maintained to **base station** (1). Thus, **encryption** communication between terminal and **base - station** is performed, through **base - station** group key.
DETAILED DESCRIPTION - Several disclosure key and **secret key** of intrinsic disclosure key system are provided to each terminal (2). The **base - station** (1) which controls communication, is connected to each terminal through **wireless** circuit.
USE - For **securing security** of **mobile** communication system.
ADVANTAGE - Since common key is changed for every transmission, safe and smooth group communication is enabled.
DESCRIPTION OF DRAWING(S) - The figure shows explanatory diagram of **mobile** communication system which applies communication procedure.
Base - station (1)
Terminal (2)
pp; 12 DwgNo 1/9
Title Terms: **MOBILE** ; COMMUNICATE; DYNAMIC; **SECURE** ; GROUP; COMMUNICATE; PROCEDURE; PERFORMANCE; **ENCRYPTION** ; COMMUNICATE; BASE; **STATION** ; TERMINAL; BASE; **STATION** ; GROUP; KEY
Derwent Class: P85; W01; W02
International Patent Class (Main): H04L-009/14
International Patent Class (Additional): G09C-001/00; H04B-007/26
File Segment: EPI; EngPI

12/5/18 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010625525 **Image available**
WPI Acc No: 1996-122478/199613
XRPX Acc No: N96-102915
Digital cordless telephone with safe secrecy key setting e.g. PHS - has second key generator which generates secrecy key based on key generation information from mobile **sub-** station
Patent Assignee: SHARP KK (SHAF)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 8018657	A	19960119	JP 94146782	A	19940628	199613	B

Priority Applications (No Type Date): JP 94146782 A 19940628
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 8018657	A		7	H04M-001/68	

Abstract (Basic): JP 8018657 A

The telephone performs **wireless** transmission in which **secret key** information is prevented from transmission. A **base station** (1) is connected to the public circuit. The **base station** and the **mobile** sub- **station** (10) carry out digital encoding of audio signal and performs **wireless** transmission mutually. A first key generation device (5) forms a **secret key** based on the key generation information which is input into the **mobile** sub- **station** by a key input device (13).

The key generation information is then transmitted to the **base station** . A control device (2) controls the encoding by the **secret key** . A second key generator (15) forms another **secret key** based on the key generation information received from the **mobile** sub- **station** . The **secret key** is then stored in a pair of key retainers (6,16).

ADVANTAGE - Prevents transmission of **secret key** . Realizes safe secrecy key. Realizes highly safe **privacy** function of secrecy key.

Dwg.1/10

Title Terms: DIGITAL; CORD; TELEPHONE; SAFE; SECRET; KEY; SET; SECOND; KEY; GENERATOR; GENERATE; SECRET; KEY; BASED; KEY; GENERATE; INFORMATION; **MOBILE** ; SUB; **STATION**
Index Terms/Additional Words: **PERSON AL_HAND** ; HANDY; TELEPHONE
Derwent Class: W01
International Patent Class (Main): H04M-001/68
International Patent Class (Additional): H04L-009/06; H04L-009/14
File Segment: EPI

12/5/19 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010307578 **Image available**
WPI Acc No: 1995-208836/199528
XRPX Acc No: N95-163659
Key distribution and authentication **for** secure **data traffic - generating network key and backbone key for remote** station **at** base station
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC); IBM CORP (IBMC)
Inventor: BAUCHOT F; BJORKLUND R E; HERZBERG A; KUTTEN S; WETTERWALD M M
Number of Countries: 006 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 658021	A1	19950614	EP 93480219	A	19931208	199528	B
CA 2130396	A	19950609	CA 2130396	A	19940818	199536	
JP 7202883	A	19950804	JP 94256367	A	19941021	199540	
US 5539824	A	19960723	US 94348656	A	19941202	199635	
CA 2130396	C	19980331	CA 2130396	A	19940818	199824	
EP 658021	B1	20010328	EP 93480219	A	19931208	200118	
DE 69330065	E	20010503	DE 630065	A	19931208	200132	
			EP 93480219	A	19931208		

Priority Applications (No Type Date): EP 93480219 A 19931208
Cited Patents: 1.Jnl.Ref; US 5199072
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 658021	A1	E	16	H04L-009/08	
Designated States (Regional): DE FR GB					
CA 2130396	A			H04L-009/08	
JP 7202883	A		16	H04L-009/06	
US 5539824	A		14	H04N-009/32	
CA 2130396	C			H04L-009/08	
EP 658021	B1	E		H04L-009/08	
Designated States (Regional): DE FR GB					
DE 69330065	E			H04L-009/08	Based on patent EP 658021

Abstract (Basic): EP 658021 A

The method of key distribution and **authentication** involves installing a common **hidden key** (Km) and a unique identifier (UA) to each **station** . In order to install one **base station** a preliminary key (K1) is generated and installed. This triggers selection of a network key (Knet) which is stored in a network manager. Another **base station** is also installed and a key is selected for it based upon that of the first **base station** .

A remote **station** is installed by choosing a name for it on the basis of its identifier. The name is **encrypted** within the installed **station** . A name parameter is computed and provided to the remote **station** where it is stored. Pref., the preliminary key is randomly generated within the network manager.

USE/ADVANTAGE - For **wireless** LAN transmission network. Easy to use since **stations** can be initiated on site. Distribution of **private keys** for LAN remote and **base stations** .

Dwg.2/6

Title Terms: KEY; DISTRIBUTE; **AUTHENTICITY** ; **SECURE** ; DATA; TRAFFIC; GENERATE; NETWORK; KEY; BACKBONE; KEY; REMOTE; **STATION** ; BASE; **STATION**
Derwent Class: W01
International Patent Class (Main): H04L-009/06; H04L-009/08; H04N-009/32
International Patent Class (Additional): H04L-009/14; H04L-009/32; H04L-012/22; H04L-012/28
File Segment: EPI

16/5/2 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015966879 **Image available**
WPI Acc No: 2004-124720/200413
XRPX Acc No: N04-099794
Resource use authorization sharing method e.g. for bank account, involves forwarding secret key **unit to server to perform partial operations on message received from slave device**
Patent Assignee: NOKIA CORP (OYNO)
Inventor: ASOKAN N; NYBERG K; SOVIO S; NIEMI V
Number of Countries: 031 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 1383265	A1	20040121	EP 200215842	A	20020716	200413 B
US 20040062400	A1	20040401	US 2003621258	A	20030715	200425

Priority Applications (No Type Date): EP 200215842 A 20020716
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1383265	A1	E	13	H04L-009/32	
Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR					
US 20040062400	A1			H04L-009/00	

Abstract (Basic): EP 1383265 A1

NOVELTY - A **secret key** (d) is split into two units (d1,d2) at a master device (11) acting as delegator of authorization. A piece of information relating to the unit (d1) is forwarded to a slave device (13) enabling the device to perform partial secret operation on a message. The unit (d2) is forwarded to a server (12) enabling the server to perform partial operations on the message received from the slave device.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) delegator;

(2) server for supporting chain delegation authorization use.

USE - For sharing authorization to use resources such as bank account among devises such as **mobile** phones, personal digital assistant (**PDA**), and personal computer.

ADVANTAGE - Since a security **connection** is **established** between the slave device and the server, the computational workload on the server is reduced, thus the capability of proposed authorization delegation to the slave device is extended in a simple way.

DESCRIPTION OF DRAWING(S) - The figure shows a chained delegation of authorization.

master device (11)

server (12)

slave device(d) secret master key (13)

secret key units (d1,d2)

pp; 13 DwgNo 2/2

Title Terms: RESOURCE; AUTHORISE; SHARE; METHOD; BANK; ACCOUNT; FORWARDING; SECRET; KEY; UNIT; SERVE; PERFORMANCE; OPERATE; MESSAGE; RECEIVE; SLAVE; DEVICE
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00; H04L-009/32
File Segment: EPI

```
Set     Items   Description
S1     361485   WIRELESS OR WIFI OR WAP OR CELLULAR? OR MOBILE OR BLUETOOT-
            H? OR WI()FI
S2       8288   (SECRET? OR PRIVATE? OR HIDDEN? OR CONCEAL?)(N)(KEY OR KEY-
            S)
S3        596   (CHANNEL? OR SELF()DISTRIBUTED)(N)(KEY OR KEYS)
S4     325619   STATION? OR PDA OR PORTABLE()DIGITAL()ASSISTANT? OR CELLPH-
            ONE? OR (CELL OR CELLULAR OR MOBILE)()(TELEPHONE? OR DEVICE? -
            OR LAPTOP? OR NOTEBOOK)
S5     103420   (CREATE? OR ESTABLISH? OR OPEN? OR GENERAT?)(2N)( ROUTE? OR
             CHANNEL? OR PATH? OR CONNECTION?)
S6          1   S1(10N)S2(10N)S3
S7        252   S1(10N)(S2 OR S3)(10N)S4
S8       7886   S1(10N)(S1 OR S)(10N)S5
S9     666671   AUTHENTIC? OR VERIF? OR SECUR? OR ENCRYPT? OR ENCIPHER? OR
            ENCYPHER? OR CRYPTOG? OR PRIVACY OR PASSWORD? OR ID OR HANDSH-
            AKE? OR CRAM OR USER()(NAME? OR IDENTIFIER?)
S10       824   (S7 OR S8)(10N)S9
S11    118672   ACCESS()POINT? OR BEACON? OR SERVER? OR BASE()STATION?
S12       299   S10(10N)S11
S13        64   S12 AND IC=(H04L-009 OR G09C-001 OR H04M)
S14        25   S13 NOT AD=20000912:20030912
S15        21   S14 NOT AD=20030912:20050901
File 348:EUROPEAN PATENTS 1978-2005/Aug W01
        (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20050811,UT=20050804
        (c) 2005 WIPO/Univentio
```

15/3,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01132330
Method and apparatus for establishing a secure connection over a one-way data path
Verfahren und Anordnung zur Herstellung sicherer Verbindungen uber Einwegskanale
Methode et appareil pour etablir des liaisons securisees sur canaux unidirectionels
PATENT ASSIGNEE:
Openwave Systems Inc., (2766843), 800 Chesapeake Drive, Redwood City, CA 94063, (US), (Proprietor designated states: all)
INVENTOR:
King, Peter F., 121 Presidio Avenue, Half Moon Bay, CA 94019, (US)
LEGAL REPRESENTATIVE:
Ablett, Graham Keith et al (53082), Ablett & Stebbing, Caparo House, 101-103 Baker Street, London W1M 1FD, (GB)
PATENT (CC, No, Kind, Date): EP 989712 A2 000329 (Basic)
EP 989712 A3 020417
EP 989712 B1 050406
APPLICATION (CC, No, Date): EP 99307459 990921;
PRIORITY (CC, No, Date): US 158317 980921
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-029/06; **H04L-009/08**
ABSTRACT WORD COUNT: 125
NOTE:
Figure number on first page: 2B

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200013	812
CLAIMS B	(English)	200514	956
CLAIMS B	(German)	200514	883
CLAIMS B	(French)	200514	1201
SPEC A	(English)	200013	9183
SPEC B	(English)	200514	9135
Total word count - document A			9997
Total word count - document B			12175
Total word count - documents A + B			22172

...INTERNATIONAL PATENT CLASS: **H04L-009/08**
...SPECIFICATION two-way data channel. As examples, both the HDTP and the WTLS protocols require a **handshake** operation between the **server** and a **mobile** device to **establish** a **secure connection** . Conventionally, the two-way data channel is needed to provide the handshake operation. As a...

...a two-way data channel; a network gateway coupled between the wired network and the **wireless** carrier network, the network gateway includes a secure connection processor that establishes a secure connection over the first channel by exchanging **security** information over the second channel; and a plurality of **wireless** **mobile** devices that can exchange data with the server computers on the wired network via the **wireless** carrier network and the network gateway. The messages are supplied from the network gateway to the **wireless** **mobile** devices over the **secure connection** **established** over the first channel.
As a **mobile** device capable of connecting to a network of computers through a **wireless** link, an embodiment of the invention includes: a display screen that displays graphics and text...

...SPECIFICATION degree)7, July 1998, page 1480-1497, represents the closiest prior art and discloses a **handshake** operation between a **server** and a **mobile** device to **establish** a **secure connection** .

One problem with the conventional approach to **establishing** a **secure connection** is that it requires a two-way data channel. As examples, both the HDTP and the WTLS protocols require a **handshake** operation between the **server** and a **mobile** device to **establish** a **secure connection** . Conventionally, the two-way data channel is needed to provide the handshake operation. As a...

...a two-way data channel; a network gateway coupled between the wired network and the **wireless** carrier network, the network gateway includes a secure connection processor that establishes a secure connection over the first channel by exchanging **security** information over the second channel; and a plurality of **wireless** **mobile** devices that can exchange data with the server computers on the wired network via the **wireless** carrier network and the network gateway. The messages are supplied from the network gateway to the **wireless** **mobile** devices over the **secure connection** **established** over the first channel.

As a **mobile** device capable of connecting to a network of computers through a **wireless** link, an embodiment of the invention includes: a display screen that displays graphics and text...

15/3,K/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00687914
A method and system for key distribution and authentication in a data communication network
Verfahren und System zur Schlusselverteilung und Authentifizierung in einem Datenubertragungssystem
Procede et systeme de distribution de cle et authentification dans un reseau de communication de donnees
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (Proprietor designated states: all)
INVENTOR:
Bjorklund, Ronald Einar, Villa "La Lezardiere", Chemin de Bezaudin 76, F-06510 Gattieres, (FR)
Bauchot, Frederic, 299 Chemin du Vallon, La Tourraque, F-06640 Saint Jeannet, (FR)
Wetterwald, Michele Marie, 32 Chemin de Saint Laurent, F-06800 Cagnes Sur Mer, (FR)
Kutten, Shay, 41 Lenox Street, Rockaway, NJ 07866, (US)
Herzberg, Amir, 3935 Blackstone Avenue, No. 4a, Bronx, NY 10471, (US)
LEGAL REPRESENTATIVE:
de Pena, Alain (15151), Compagnie IBM France Departement de Propriete Intellectuelle, 06610 La Gaude, (FR)
PATENT (CC, No, Kind, Date): EP 658021 A1 950614 (Basic)
EP 658021 B1 010328
APPLICATION (CC, No, Date): EP 93480219 931208;
PRIORITY (CC, No, Date): EP 93480219 931208
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **H04L-009/08** ; **H04L-009/32**
ABSTRACT WORD COUNT: 161
NOTE:
Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB95	904
CLAIMS B	(English)	200113	878
CLAIMS B	(German)	200113	817
CLAIMS B	(French)	200113	1096
SPEC A	(English)	EPAB95	3678
SPEC B	(English)	200113	3720
Total word count - document A			4583
Total word count - document B			6511
Total word count - documents A + B			11094

INTERNATIONAL PATENT CLASS: **H04L-009/08** ...

... **H04L-009/32**

...SPECIFICATION Another object of this invention is to provide such a method for a so-called **wireless** LAN network combining both **wireless** communications with wired LAN.
Still another object of this invention is to provide a method for distributing **private keys** needed in an **authentication** procedure of a **wireless** LAN remote and **base stations** .
These and other characteristics, objects and advantages of this invention will become more apparent from...

...SPECIFICATION Another object of this invention is to provide such a method for a so-called **wireless** LAN network combining both **wireless** communications with wired LAN.

Still another object of this invention is to provide a method for distributing **private keys** needed in an **authentication** procedure of a **wireless** LAN remote and **base stations** .

These and other characteristics, objects and advantages of this invention will become more apparent from...

15/3,K/21 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00196992
A METHOD OF CARRYING OUT AN AUTHENTICATION CHECK BETWEEN A BASE STATION AND A MOBILE STATION IN A MOBILE RADIO SYSTEM
PROCEDE D'EXECUTION D'UN CONTROLE D'AUTHENTIFICATION ENTRE UNE STATION DE BASE ET UNE STATION MOBILE DANS UN SYSTEME DE RADIO MOBILE
Patent Applicant/Assignee:
TELEFONAKTIEBOLAGET LM ERICSSON,
Inventor(s):
WILKINSON Dent Paul,
RAITH Alex Krister,
DAHLIN Jan Erik Ake Steinar,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9114348 A1 19910919
Application: WO 91SE66 19910129 (PCT/WO SE9100066)
Priority Application: SE 90856 19900309
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AU BR CA FI JP KR NO
Publication Language: English
Fulltext Word Count: 2444
International Patent Class: **H04M-01:66**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... formed
values of Resp 3. If the values coincide, connection of the call continues to **establish** a speech **connection** .

The method steps according to block 7, 8 and 9 provide an authenti cation check in which the **mobile** decides whether or not the **base station** is **authentic** , since **verif** ication of the signal Resp 2 sent from the **base station** takes place in the mobile, and against a value Resp 2 calculated in said mobile...

...2, 3 and 4 can be
carried out on a general control channel in the **mobile** radio system, and the **authentication** check according to blocks 7-12 can be carried out on the speech **channel established** between the **base station** BS and the **mobile** MSk (blocks 5 and 6) e
Figure 4 is a block diagram illustrating the f...

```
Set     Items   Description
S1    1346057   WIRELESS OR WIFI OR WAP OR CELLULAR? OR MOBILE OR BLUETOOTH? OR WI()FI
FROM 8, 35, 56, 57, 65, 2, 94, 111, 6, 144, 34, 62, 99, 95
S2       5815   (SECRET? OR PRIVATE? OR HIDDEN? OR CONCEAL?)(N)(KEY OR KEYS) FROM 8, 35,
56, 57, 65, 2, 94, 111, 6, 144, 34, 62, 99, 95
S3        185   (CHANNEL? OR SELF()DISTRIBUTED)(N)(KEY OR KEYS) FROM 8, 35, 56, 57, 65, 2,
94, 111, 6, 144, 34, 62, 99, 95
S4     966584   STATION? OR PDA OR PORTABLE()DIGITAL()ASSISTANT? OR CELLPHONE? OR (CELL OR
CELLULAR OR MOBILE)()(TELEPHONE? OR DEVICE? OR LAPTOP? OR NOTEBOOK) FROM 8, 35, 56, 57,
65, 2, 94, 111, 6, 144, 34, 62, 99, 95
S5       90144   (CREATE? OR ESTABLISH? OR OPEN? OR GENERAT?)(2N)( ROUTE? OR CHANNEL? OR
PATH? OR CONNECTION?) FROM 8, 35, 56, 57, 65, 2, 94, 111, 6, 144, 34, 62, 99, 95
S6           0   S1(10N)S2(10N)S3 FROM 8, 35, 56, 57, 65, 2, 94, 111, 6, 144, 34, 62, 99,
95
S7          12   S1(10N)(S2 OR S3)(10N)S4 FROM 8, 35, 56, 57, 65, 2, 94, 111, 6, 144, 34,
62, 99, 95
S8        1828   S1(10N)(S1 OR S)(10N)S5 FROM 8, 35, 56, 57, 65, 2, 94, 111, 6, 144, 34,
62, 99, 95
S9     1975038   AUTHENTIC? OR VERIF? OR SECUR? OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR
CRYPTOG? OR PRIVACY OR PASSWORD? OR ID OR HANDSHAKE? OR CRAM OR USER()(NAME? OR
IDENTIFIER?) FROM 8, 35, 56, 57, 65, 2, 94, 111, 6, 144, 34, 62, 99, 95
S10         63   (S7 OR S8)(10N)S9 FROM 8, 35, 56, 57, 65, 2, 94, 111, 6, 144, 34, 62, 99,
95
S11     218659   ACCESS()POINT? OR BEACON? OR SERVER? OR BASE()STATION? FROM 8, 35, 56, 57,
65, 2, 94, 111, 6, 144, 34, 62, 99, 95
S12          4   S10(10N)S11 FROM 8, 35, 56, 57, 65, 2, 94, 111, 6, 144, 34, 62, 99, 95
S13          0   S S1 AND S2 AND S3 AND S4
S14          0   S S1 AND (S2 OR S3) AND S4 AND S5 AND S9 AND S10
S15          0   S S1 AND (S2 OR S3) AND S4 AND S5
S16         69   S S7 OR S10 OR S12
S17         48   S S16 AND S11
S18          7   S S17 NOT PY>2000
 ; show files
```

[File 8] **Ei Compendex(R)** 1970-2005/Aug W1

[File 35] **Dissertation Abs Online** 1861-2005/Jul

[File 56] **Computer and Information Systems Abstracts** 1966-2005/Jul

[File 57] **Electronics & Communications Abstracts** 1966-2005/Jul

[File 65] **Inside Conferences** 1993-2005/Aug W2

[File 2] **INSPEC** 1969-2005/Aug W1

[File 94] **JICST-EPlus** 1985-2005/Jun W4

[File 111] **TGG Natl.Newspaper Index(SM)** 1979-2005/Aug 16

[File 6] **NTIS** 1964-2005/Aug W1

[File 144] **Pascal** 1973-2005/Aug W1

[File 34] **SciSearch(R) Cited Ref Sci** 1990-2005/Aug W1

[File 62] **SPIN(R)** 1975-2005/Jun W1

[File 99] **Wilson Appl. Sci & Tech Abs** 1983-2005/Jul

[File 95] **TEME-Technology & Management** 1989-2005/Jul W2

**File 95: Customers in Germany, Austria, and Switzerland should contact their local Dialog representative.*

```
Set     Items   Description
S1     100835   WIRELESS OR WIFI OR WAP OR CELLULAR? OR MOBILE OR BLUETOOTH? OR WI()FI
FROM 696
S2        177   (SECRET? OR PRIVATE? OR HIDDEN? OR CONCEAL?)(N)(KEY OR KEYS) FROM 696
S3         29   (CHANNEL? OR SELF()DISTRIBUTED)(N)(KEY OR KEYS) FROM 696
S4      40511   STATION? OR PDA OR PORTABLE()DIGITAL()ASSISTANT? OR CELLPHONE? OR (CELL OR
CELLULAR OR MOBILE)()(TELEPHONE? OR DEVICE? OR LAPTOP? OR NOTEBOOK) FROM 696
S5       1521   (CREATE? OR ESTABLISH? OR OPEN? OR GENERAT?)(2N)( ROUTE? OR CHANNEL? OR
PATH? OR CONNECTION?) FROM 696
S6          0   S1(10N)S2(10N)S3 FROM 696
S7          2   S1(10N)(S2 OR S3)(10N)S4 FROM 696
S8        110   S1(10N)(S1 OR S)(10N)S5 FROM 696
S9      43618   AUTHENTIC? OR VERIF? OR SECUR? OR ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR
CRYPTOG? OR PRIVACY OR PASSWORD? OR ID OR HANDSHAKE? OR CRAM OR USER()(NAME? OR
IDENTIFIER?) FROM 696
S10         5   (S7 OR S8)(10N)S9 FROM 696
S11     15364   ACCESS()POINT? OR BEACON? OR SERVER? OR BASE()STATION? FROM 696
S12         4   S10(10N)S11 FROM 696
S13        17   S S8(S)S9
S14        16   S S8(S)S11
S15        27   S S7 OR S13 OR S10 OR S12 OR S14
S16        25   RD (unique items)
S17        15   S S16 NOT PY>2000
 ; show files
```

[File 696] **DIALOG Telecom. Newsletters** 1995-2005/Aug 16

```
S1    3604621   WIRELESS OR WIFI OR WI()FI OR CELLULAR OR MOBILE OR BLUETO-
            OTH OR WAP
S2          89   DYNAMIC()SESSION()KEY? ?
S3           0   INDEPENDENTLY()GENERATED()KEY? ?
S4         250   LEAP()PROTOCOL OR EAP(2N)CISCO
S5        9592   S1 (12N) (LEAP OR WEP()ENHANCEMENT?)
S6           0   S1 (12N) (INDEPENDENT?)()(CREAT? OR GENERAT? OR SPAWN? OR -
            MAKE OR BUILD? OR ASSEMBL? OR AUTHOR OR AUTHORING)()(KEY OR K-
            EYS)
S7          32   S1 (12N) (DYNAMIC? OR ADAPT? OR CHANG? OR MODIF? OR ALTER?-
            )()SESSION?
S8         705   S5(12N)(KEY OR KEYS OR SECUR? OR CRYPTOG? OR ENCRYPT? OR E-
            NCIPHER? OR ENCYPHER? OR CYPHER? OR CIPHER? OR CRAM OR CHALLE-
            NGE? OR PIN OR PASSWORD? OR IDENTIFIER? OR ID)
S9          76   S1(12N)S4
S10         56   S8(12N)(DYNAMIC? OR INDEPENDENT? OR DISTRIBUT? OR REDISTRI-
            BUT?)
S11        399   S2 OR S4 OR S7 OR S9 OR S10
S12         77   S11 NOT PY>2000
S13         34   RD (unique items)
File 275:Gale Group Computer DB(TM) 1983-2005/Aug 18
         (c) 2005 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2005/Aug 18
         (c) 2005 The Gale group
File  75:TGG Management Contents(R) 86-2005/Aug W1
         (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Aug 17
         (c) 2005 The Gale Group
File  16:Gale Group PROMT(R) 1990-2005/Aug 17
         (c) 2005 The Gale Group
File 624:McGraw-Hill Publications 1985-2005/Aug 17
         (c) 2005 McGraw-Hill Co. Inc
File 484:Periodical Abs Plustext 1986-2005/Aug W2
         (c) 2005 ProQuest
File 613:PR Newswire 1999-2005/Aug 18
         (c) 2005 PR Newswire Association Inc
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 141:Readers Guide 1983-2004/Dec
         (c) 2005 The HW Wilson Co
File 239:Mathsci 1940-2005/Oct
         (c) 2005 American Mathematical Society
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File 696:DIALOG Telecom. Newsletters 1995-2005/Aug 17
         (c) 2005 Dialog
File 553:Wilson Bus. Abs. FullText 1982-2004/Dec
         (c) 2005 The HW Wilson Co
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Aug 18
         (c) 2005 The Gale Group
File 674:Computer News Fulltext 1989-2005/Aug W1
         (c) 2005 IDG Communications
File  88:Gale Group Business A.R.T.S. 1976-2005/Aug 17
         (c) 2005 The Gale Group
File 369:New Scientist 1994-2005/May W5
         (c) 2005 Reed Business Information Ltd.
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 635:Business Dateline(R) 1985-2005/Aug 17
         (c) 2005 ProQuest Info&Learning
File  15:ABI/Inform(R) 1971-2005/Aug 17
         (c) 2005 ProQuest Info&Learning
File   9:Business & Industry(R) Jul/1994-2005/Aug 17
         (c) 2005  The Gale Group
File  13:BAMP 2005/Aug W1
```

File 810:Business Wire 1986-1999/Feb 28

File 610:Business Wire 1999-2005/Aug 18

File 647:CMP Computer Fulltext 1988-2005/Jul W5

File 98:General Sci Abs/Full-Text 1984-2004/Dec

File 148:Gale Group Trade & Industry DB 1976-2005/Aug 18

File 634:San Jose Mercury Jun 1985-2005/Aug 16

13/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01916318 SUPPLIER NUMBER: 18093288 (USE FORMAT 7 OR 9 FOR FULL TEXT)
GEIS aims to stimulate EDI growth. (General Electric Information Services) (Company Business and Marketing)
Sterlicchi, John
MIDRANGE Systems, v9, n3, p31(2)
March 15, 1996
ISSN: 1041-8237 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 583 LINE COUNT: 00050

... environment to permit secure transmission of highly sensitive data over the Internet. It provides a **dynamic session key** that encrypts the session itself to secure all information passed from sender to receiver.
InterBusiness...

13/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01906543 SUPPLIER NUMBER: 18031851 (USE FORMAT 7 OR 9 FOR FULL TEXT)
E-mail: GE Information Services selects Post.Office E-mail server software to be part of GE interbusiness strategy. (Software.com product adopted) (Product Information)
EDGE: Work-Group Computing Report, v7, n302, p18(1)
Feb 26, 1996
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 490 LINE COUNT: 00049

... the Internet with verification and authentication for private transactions."

GE INTERBUSINESS

GE InterBusiness combines encrypted **dynamic session key** , mutual authentication, and advanced firewall technology. It is based on standard Internet protocols and establishes...

13/3,K/7 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04747600 Supplier Number: 63945120 (USE FORMAT 7 FOR FULLTEXT)
Mercury Interactive introduces testing and monitoring solutions to improve performance and reliability of wireless web applications; Nokia, AvantGo, Brience, Everypath, Inc. and six solution providers team with Mercury Interactive to ensure scalable, reliable wireless web applications.
M2 Presswire, pNA
August 8, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1954

... order to comply with micro-browser, gateway, and vendor-specific features such as dynamic content, **dynamic** session identifiers and cookies.

Mercury Interactive's LoadRunner and ActiveTest stress customers' **WAP** and i-mode applications by emulating thousands of wireless micro-browser user sessions in order...

13/3,K/34 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

08458617 SUPPLIER NUMBER: 17984181 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Pipeline. (Internet) (News Briefs)
InfoWorld, v18, n7, p53(1)
Feb 12, 1996
ISSN: 0199-6649 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 239 LINE COUNT: 00025

... commerce offering that provides security for business transactions over the Internet. GE InterBusiness combines encrypted **dynamic session - key** , mutual authentication, and advanced firewall technology, establishing a secure pipeline for users to conduct electronic..

```
S1    1390547   WIRELESS OR WIFI OR WI()FI OR CELLULAR OR MOBILE OR BLUETO-
            OTH OR WAP
S2          4   DYNAMIC()SESSION()KEY? ?
S3          0   INDEPENDENTLY()GENERATED()KEY? ?
S4          8   LEAP()PROTOCOL OR EAP(2N)CISCO
S5        630   S1  AND (LEAP OR WEP()ENHANCEMENT?)
S6          0   S1  AND (INDEPENDENT?)()(CREAT? OR GENERAT? OR SPAWN? OR M-
            AKE OR BUILD? OR ASSEMBL? OR AUTHOR OR AUTHORING)()(KEY OR KE-
            YS)
S7         13   S1  AND (DYNAMIC? OR ADAPT? OR CHANG? OR MODIF? OR ALTER?)-
            ()SESSION?
S8         30   S5 AND (SECURE? OR KEY? ? OR IDENTIFIER? OR SESSIONKEY? OR
            PRIVATEKEY? OR PUBLICKEY? OR KEYEXCHANGE?)
S9         30   S5 AND (ENCRYPT? OR ENCIPHER? OR CYPHER? OR CIPHER? OR CRAM
             OR CHALLENGE? OR HANDSHAKE? OR AUTHENTIC? OR AUTHORI?)
S10        80   S2 OR S4 OR S7 OR S8 OR S9
S11        56   RD (unique items)
S12        26   S11 NOT PY>2000
File   8:Ei Compendex(R) 1970-2005/Aug W1
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Jul
         (c) 2005 ProQuest Info&Learning
File  56:Computer and Information Systems Abstracts 1966-2005/Jul
         (c) 2005 CSA.
File  57:Electronics & Communications Abstracts 1966-2005/Jul
         (c) 2005 CSA.
File  65:Inside Conferences 1993-2005/Aug W2
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Aug W1
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Jun W4
         (c)2005 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2005/Aug 17
         (c) 2005 The Gale Group
File   6:NTIS 1964-2005/Aug W1
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Aug W1
         (c) 2005 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Aug W2
         (c) 2005 Inst for Sci Info
File  62:SPIN(R) 1975-2005/Jun W1
         (c) 2005 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jul
         (c) 2005 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2005/Jul W2
         (c) 2005 FIZ TECHNIK
```

12/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

08515655 E.I. No: EIP01035587292
Title: Guarantee of QoS for wireless **multimedia streams based on** adaptive session
Author: Zhang, Zhanjun; Han, Chengde; Yang, Xueliang
Corporate Source: Chinese Acad of Science, Beijing, China
Conference Title: 2000 IEEE International Conference on Personal Wireless Communications
Conference Location: Hyderabad, India Conference Date: 20001217-20001220
Sponsor: IEEE; University of Victoria
E.I. Conference No.: 57970
Source: IEEE International Conference on Personal Wireless Communications 2000. IEEE, Piscataway, NJ, USA,00TH8488. p 283-287
Publication Year: 2000
CODEN: 85QVA4
Language: English
Document Type: CA; (Conference Article) Treatment: A; (Applications); T ; (Theoretical)
Journal Announcement: 0105W1
Abstract: The guarantee of quality of service (QoS) is a key issue for multimedia streams in **wireless** multimedia communications. QoS parameters required by most of multimedia streams are ranges or in set, left bracket QoS//m//i//n, QoS//m//a//x right bracket . Computer systems and network systems must allocate enough resources such as CPU, I/O, memory and bandwidth to meet these QoS parameters. These resources are dynamic variations in availability e.g. bandwidth on radio during multimedia streams transmission. The **adaptive session** is defined to formularize multimedia stream in this paper. It can allocate resources with QoS//m//i//n during establishment of multimedia stream call and it can dynamic adjust its QoS parameters in left bracket QoS//m//i//n, QoS//m//a//x right bracket by PID to adapt the variations in resource availability during multimedia transmission. It not only meets the QoS parameters required, but also improves the useful of resources. (Author abstract) 4 Refs.
Descriptors: *Frequency allocation; Multimedia systems; Quality of service; **Wireless** telecommunication systems; Computer hardware; Radio; Resource allocation; Bandwidth; Algorithms; Theorem proving
Identifiers: **Wireless** multimedia streams; Multimedia stream transmission; Producer-consumer model
Classification Codes:
716.3 (Radio Systems & Equipment); 716.4 (Television Systems & Equipment); 723.5 (Computer Applications); 716.1 (Information & Communication Theory); 722.1 (Data Storage, Equipment & Techniques); 912.2 (Management)
716 (Radar, Radio & TV Electronic Equipment); 723 (Computer Software); 722 (Computer Hardware); 912 (Industrial Engineering & Management)
71 (ELECTRONICS & COMMUNICATIONS); 72 (COMPUTERS & DATA PROCESSING); 91 (ENGINEERING MANAGEMENT)

12/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06298866 E.I. No: EIP03087365083
Title: Proceedings of the 4th internation workshop on discrete algorithms and methods for mobile **computing and communications**
Author: Anon (Ed.)
Conference Title: Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications
Conference Location: Boston, MA, United States Conference Date: 20000811-20000811
Sponsor: ACM SIGMOBILE; National Science Foundation; Basic and Appl. Simul. Science Group of Los Alamos Nat. Lab.
E.I. Conference No.: 60386
Source: Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications 2000.
Publication Year: 2000
ISBN: 1581133014
Language: English
Document Type: CP; (Conference Review) Treatment: T; (Theoretical)
Journal Announcement: 0302W4
Abstract: The proceedings contains 12 papers from the Conference of the 4th International Workshop on Discrete Algorithms and Methods for **Mobile** Computing and Communications. Topics discussed include: on-line algorithms for the channel assignment in **cellular** networks, energy efficient routing in radio networks; **mobile** facility location; and **dynamic session** management for static and **mobile** users: a competitive on-line algorithmic approach. (Edited abstract)
Descriptors: *Telecommunication networks; Channel capacity; Bandwidth; Signal interference; Transmitters; Signal to noise ratio; Energy efficiency ; Natural frequencies; Data structures; Network protocols; Telecommunication traffic; **Mobile** computing; HTTP
Identifiers: **Cellular** networks; Channel assignment; Call allocation algorithms; Radio networks (RN); **Mobile** facility location; **Wireless** ad hoc networks; Internet industry; Virtual channels (VC); Tag identification; EiRev
Classification Codes:
716.1 (Information & Communication Theory); 723.2 (Data Processing); 921.4 (Combinatorial Mathematics, Includes Graph Theory, Set Theory)
716 (Electronic Equipment, Radar, Radio & Television); 723 (Computer Software, Data Handling & Applications); 921 (Applied Mathematics)
71 (ELECTRONICS & COMMUNICATION ENGINEERING); 72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

12/5/9 (Item 9 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04113373 E.I. No: EIP95032626418
Title: Building a secure communications network
Author: Erman, Timothy
Corporate Source: TeleSec
Source: Telecommunications (Americas Edition) v 29 n 2 Feb 1995. 3pp
Publication Year: 1995
CODEN: TLCMDV ISSN: 0278-4831
Language: English
Document Type: JA; (Journal Article) Treatment: A; (Applications)
Journal Announcement: 9505W3
Abstract: Achieving network security requires more than simply selecting a system that utilizes good encryption algorithm. Several algorithm (data encrypted left bracket DES right bracket , RSA, Skipjack, Kerberos, and so on) are capable of providing excellent information security. However, the most robust of encryption algorithms is of no value without proper system implementation and user security awareness. Any security system will be attacked at its weakest point. Thus, in order to have effective data communication security, the network security system must be architecturally sound and all users must adhere to the system security policies.
Descriptors: *Telecommunication networks; Security of data; Local area networks; Information services; Computer systems; Modems; Cryptography; Data communication systems; Algorithms; Security systems
Identifiers: Secure communication networks; Security policy; Crypto algorithms; **Dynamic session keys** ; Key encryption keys; Random authentication variables
Classification Codes:
723.2 (Data Processing); 722.3 (Data Communication, Equipment & Techniques); 903.4 (Information Services); 722.4 (Digital Computers & Systems); 723.1 (Computer Programming)
716 (Radar, Radio & TV Electronic Equipment); 723 (Computer Software); 722 (Computer Hardware); 903 (Information Science)
71 (ELECTRONICS & COMMUNICATIONS); 72 (COMPUTERS & DATA PROCESSING); 90 (GENERAL ENGINEERING)

```
Set     Items   Description
S1        508   (LEAP(N)(CISCO) OR EAP(N)CISCO OR LEAP()PROTOCOL)
S2         18   S1 NOT PY>2000
S3          6   RD (unique items)
File   2:INSPEC 1969-2005/Aug W1
         (c) 2005 Institution of Electrical Engineers
File   8:Ei Compendex(R) 1970-2005/Aug W1
         (c) 2005 Elsevier Eng.  Info. Inc.
File   9:Business & Industry(R) Jul/1994-2005/Aug 17
         (c) 2005  The Gale Group
File  13:BAMP 2005/Aug W1
         (c) 2005  The Gale Group
File  15:ABI/Inform(R) 1971-2005/Aug 17
         (c) 2005 ProQuest Info&Learning
File  16:Gale Group PROMT(R) 1990-2005/Aug 17
         (c) 2005 The Gale Group
File  20:Dialog Global Reporter 1997-2005/Aug 18
         (c) 2005 Dialog
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Aug W2
         (c) 2005 Inst for Sci Info
File  47:Gale Group Magazine DB(TM) 1959-2005/Aug 18
         (c) 2005 The Gale group
File  88:Gale Group Business A.R.T.S. 1976-2005/Aug 17
         (c) 2005 The Gale Group
File  95:TEME-Technology & Management 1989-2005/Jul W2
         (c) 2005 FIZ TECHNIK
File 111:TGG Natl.Newspaper Index(SM) 1979-2005/Aug 17
         (c) 2005 The Gale Group
File 144:Pascal 1973-2005/Aug W1
         (c) 2005 INIST/CNRS
File 148:Gale Group Trade & Industry DB 1976-2005/Aug 18
         (c)2005 The Gale Group
File 194:FBODaily 1982/Dec-2005/May
         (c) format only 2005 Dialog
File 211:Gale Group Newsearch(TM) 2005/Aug 18
         (c) 2005 The Gale Group
File 256:TecInfoSource 82-2005/Jul
         (c) 2005 Info.Sources Inc
File 262:CBCA Fulltext 1982-2005/Aug 15
         (c) 2005 Micromedia Ltd.
File 275:Gale Group Computer DB(TM) 1983-2005/Aug 18
         (c) 2005 The Gale Group
File 349:PCT FULLTEXT 1979-2005/UB=20050811,UT=20050804
         (c) 2005 WIPO/Univentio
File 440:Current Contents Search(R) 1990-2005/Aug 18
         (c) 2005 Inst for Sci Info
File 484:Periodical Abs Plustext 1986-2005/Aug W2
         (c) 2005 ProQuest
File 545:Investext(R) 1982-2005/Aug 17
         (c) 2005 Thomson Financial Networks
File 610:Business Wire 1999-2005/Aug 18
         (c) 2005 Business Wire.
File 613:PR Newswire 1999-2005/Aug 18
         (c) 2005 PR Newswire Association Inc
File 619:Asia Intelligence Wire 1995-2005/Aug 15
         (c) 2005 Fin. Times Ltd
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Aug 18
         (c) 2005 The Gale Group
File 635:Business Dateline(R) 1985-2005/Aug 17
         (c) 2005 ProQuest Info&Learning
File 636:Gale Group Newsletter DB(TM) 1987-2005/Aug 17
         (c) 2005 The Gale Group
File 647:CMP  Computer Fulltext 1988-2005/Jul W5
         (c) 2005 CMP Media, LLC
File 649:Gale Group Newswire ASAP(TM) 2005/Aug 08
```

(c) 2005 The Gale Group
File 654:US Pat.Full. 1976-2005/Aug 16
(c) Format only 2005 Dialog
File 674:Computer News Fulltext 1989-2005/Aug W1
(c) 2005 IDG Communications
File 707:The Seattle Times 1989-2005/Aug 16
(c) 2005 Seattle Times
File 759:Business Insights 1992-2005/Aug
(c) 2005 Datamonitor
File 767:Frost & Sullivan Market Eng 2005/Aug
(c) 2005 Frost & Sullivan Inc.
File 990:NewsRoom Current May 1 -2005/Aug 18
(c) 2005 Dialog
File 991:NewsRoom 2005 Jan 1-2005/Mar 30
(c) 2005 Dialog
File 992:NewsRoom 2004 Jan 1-2004/Dec 31
(c) 2005 Dialog
File 993:NewsRoom 2003
(c) 2005 Dialog
File 994:NewsRoom 2002
(c) 2005 Dialog
File 995:NewsRoom 2001
(c) 2005 Dialog

3/5,K/5 (Item 1 from file: 256)
DIALOG(R)File 256:TecInfoSource

00145955 DOCUMENT TYPE: Review

PRODUCT NAMES: SOA (Service Oriented Architectures) (805921); EAP (Extensible Authentication Protocol) (805939); PEAP (Protected EAP) (805955)

TITLE: Security alphabet soup: What WLAN security method is best for you?
AUTHOR: Snow, Stephen
SOURCE: Frontline Solutions, v4 n2 p34(2) Feb 2003
ISSN: 0890-9768
HOMEPAGE: http://www.frontline.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Vendors are adding EAP (Extensible Authentication Protocol) types include EAP-MD-5 Challenge, EAP-Transport Layer Security (TLS), and EAP-Tunneled Transport Layer Security (EA-TTLS) authentication types to possibly provide a better method for securing a wireless LAN (WLAN) connection to their solutions. LEAP (Lightweight EAP), which is also known as **EAP - Cisco** Wireless, and PEAP (Protected EAP) are also available; Microsoft, Cisco, and RSA Security developed PEAP to secure transport of authentication data, including legacy password- based ports over 802.11 networks. LEAP is an EAP authentication type used mostly in Aironet WLANS from Cisco and can work with existing legacy operating systems and clients. LEAP has been licensed to other manufacturers. and LEAP's availability should widen soon. Wi- Fi Protected Access (WPA) is an interim security solution based on IEEE standards that is designed to work with products on the market currently. WPA will be included in Wi-Fi Certified products beginning in 2003. EAP-MD-5 Challenge is the oldest EAP authentication type. It serves as a base level of support for 802.1x devices, but is not recommended for WLANs. EAP-TLS supports certificate-based and mutual authentication of the client and the network. EAP-TTLS was developed as an extension of EAP-TLS and supports certificate-based, mutual authentication of the client and network through an encrypted channel and a way to derive dynamic, per-user, per-session WEP keys.

COMPANY NAME: Vendor Independent (999999)
DESCRIPTORS: Communications Protocols; Computer Security; LANs; Network Administration; Network Software; System Monitoring; Wireless Networks
REVISION DATE: 20031030
...wireless LAN (WLAN) connection to their solutions. LEAP (Lightweight EAP), which is also known as **EAP - Cisco** Wireless, and PEAP (Protected EAP) are also available; Microsoft, Cisco, and RSA Security developed PEAP
...

```
Set     Items   Description
S1     361053   WIRELESS OR WIFI OR WI()FI OR CELLULAR OR MOBILE OR BLUETO-
            OTH OR WAP
S2          7   DYNAMIC()SESSION()KEY? ?
S3          4   INDEPENDENTLY()GENERATED()KEY? ?
S4          6   LEAP()PROTOCOL OR EAP(2N)CISCO
S5         48   S1 (12N) (LEAP OR WEP()ENHANCEMENT?)
S6          0   S1 (12N) (INDEPENDENT?)()(CREAT? OR GENERAT? OR SPAWN? OR -
             MAKE OR BUILD? OR ASSEMBL? OR AUTHOR OR AUTHORING)()(KEY OR K-
             EYS)
S7         11   S1 (12N) (DYNAMIC? OR ADAPT? OR CHANG? OR MODIF? OR ALTER?-
             )()SESSION?
S8         72   S2 OR S3 OR S4 OR S5 OR S7
S9         54   S8 AND IC=(G06F OR H04L OR H04M OR H04N)
S10         9   S9 NOT AD=20000912:20030912
S11         3   S10 NOT AD=20030912:20050912
File 348:EUROPEAN PATENTS 1978-2005/Aug W01
         (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20050811,UT=20050804
         (c) 2005 WIPO/Univentio
```

11/3,K/2 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00518261 **Image available**
CRYPTOGRAPHIC KEY-RECOVERY MECHANISM
MECANISME D'EXTRACTION DE CLE CRYPTOGRAPHIQUE
Patent Applicant/Assignee:
FORTRESS TECHNOLOGIES INC,
FRIEDMAN Aharon,
BOZOKI Eva,
Inventor(s):
FRIEDMAN Aharon,
BOZOKI Eva,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9949613 A1 19990930
Application: WO 99US3665 19990219 (PCT/WO US9903665)
Priority Application: US 9875330 19980220
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 4615

Main International Patent Class: **H04L-009/08**
Fulltext Availability:
Detailed Description

English Abstract
...recording of any session (70). From Sidyn(t) and Pjdyn(t) one can calculate the **dynamic session key** between the two nodes (Ki,jdyn(t)) (75). However, all other parties are still protected...

Detailed Description
... a key recovery authority (KRA) and every pair of nodes share a permanent and a **dynamic session key** with each other. When two nodes initiate communication, the nodes exchange dynamic public keys (encrypted ...a recording of any session. From Sid"(0 and Pjd"(t) one can calculate the **dynamic session key** between the two nodes (K,.,d1'(t)). However, all other parties are still protected since...of any session. From
13
S:4n(t) and P."'(t) one can calculate the **dyn**amic session key between the two nodes However, all other parties are still protected since their dynamic public...

```
Set     Items   Description
S1     385331   WIRELESS OR WIFI OR WI()FI OR CELLULAR OR MOBILE OR BLUETO-
            OTH OR WAP
S2          1   DYNAMIC()SESSION()KEY? ?
S3          0   INDEPENDENTLY()GENERATED()KEY? ?
S4          0   LEAP()PROTOCOL OR EAP()CISCO
S5         11   S1 AND (LEAP OR WEP()ENHANCEMENT?)
S6          0   S1 AND (INDEPENDENT?)()(CREAT? OR GENERAT? OR SPAWN? OR MA-
             KE OR BUILD? OR ASSEMBL? OR AUTHOR OR AUTHORING)()(KEY OR KEY-
             S)
S7         10   S1 AND (DYNAMIC? OR ADAPT? OR CHANG? OR MODIF? OR ALTER?)(-
            )SESSION?
S8         22   S2 OR S5 OR S7
S9         22   IDPAT (sorted in duplicate/non-duplicate order)
S10        22   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2005/Apr(Updated 050801)
        (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200552
        (c) 2005  Thomson Derwent
```

10/5/7 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005 Thomson Derwent. All rts. reserv.

016044312 **Image available**
WPI Acc No: 2004-202163/200419
XRPX Acc No: N04-160700
Password authentication method for wireless **device, involves authenticating client using message digest 4 hashed password, where authentication request data has non-message digest 4 hashed password**
Patent Assignee: CISCO TECHNOLOGY INC (CISC-N); HALASZ D E (HALA-I); ZORN G W (ZORN-I)
Inventor: HALASZ D; ZORN G; HALASZ D E; ZORN G W
Number of Countries: 104 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20040019786	A1	20040129	US 200117544	A	20011214	200419 B
			US 2002270843	A	20021014	
WO 200436864	A2	20040429	WO 2003US32551	A	20031014	200429
AU 2003284144	A1	20040504	AU 2003284144	A	20031014	200467
EP 1552664	A2	20050713	EP 2003776375	A	20031014	200546
			WO 2003US32551	A	20031014	

Priority Applications (No Type Date): US 2002270843 A 20021014; US 200117544 A 20011214
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040019786	A1		35	H04L-009/00	CIP of application US 200117544
WO 200436864	A2	E		H04L-029/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW

AU 2003284144	A1			H04L-029/00	Based on patent WO 200436864
EP 1552664	A2	E		H04L-029/06	Based on patent WO 200436864

Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

Abstract (Basic): US 20040019786 A1
NOVELTY - An alternatively-hashed user unicode password associated with a client user name, is retrieved. A message digest 4 (MD4) hash of the user password is performed, to create an MD4 hashed password. The client is authenticated through lightweight extensible authentication protocol (**LEAP**) using MD4 hashed password, where authentication request data has non-MD4 hashed password.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(1) password authentication program;
(2) recorded medium storing password authentication program;
(3) non-MD4 encoding client authentication method;
(4) authentication server;
(5) network; and
(6) 802.11 compatible client.
USE - For password authentication in lightweight extensible authentication protocol (**LEAP**) for operating **wireless** device.
ADVANTAGE - Provides an alternative database on the network, such that the authentication server can access the alternative database during the lightweight extensible authentication process.
DESCRIPTION OF DRAWING(S) - The figures show the flow diagram of the **LEAP** encryption process.
pp; 35 DwgNo 4a, 4b/11

Title Terms: PASSWORD; AUTHENTICITY; METHOD; **WIRELESS** ; DEVICE; AUTHENTICITY; CLIENT; MESSAGE; DIGEST; HASH; PASSWORD; AUTHENTICITY; REQUEST; DATA; NON; MESSAGE; DIGEST; HASH; PASSWORD
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00; H04L-029/00; H04L-029/06
International Patent Class (Additional): H04L-012/22
File Segment: EPI

10/5/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014756344 **Image available**
WPI Acc No: 2002-577048/200262
XRPX Acc No: N02-457549

Transaction authentication method between terminal and smartcard for bus system, involves transmitting random session key between terminal and smartcard for authenticating valid smartcard and valid terminal

Patent Assignee: MOTOROLA INC (MOTI)
Inventor: LIN B; NEROT S C
Number of Countries: 026 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1223565	A1	20020717	EP 2001400091	A	20010112	200262	B

Priority Applications (No Type Date): EP 2001400091 A 20010112
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1223565	A1	E	31	G07F-007/10	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): EP 1223565 A1

NOVELTY - A random session key is transmitted between a terminal (102) and a smartcard (104). A card key (Kd) equal to the card key of the smartcard is generated at the terminal based on the key to authenticate a valid smartcard. A terminal identifier which is equal to terminal identifier of the transaction terminal is generated at the smartcard based on the key to authenticate a valid terminal.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Smartcard;
(2) Terminal;
(3) Smartcard command set;
(4) Session key generation method;
(5) **Dynamic session key** ;
(6) Set of instructions used in transaction process;
(7) Commit command;
(8) Roll-back mechanism; and
(9) Integrated circuit.

USE - For mutually authenticating transaction in public transport system such as train or bus system, in fare or debit-based application such as parking and taxis.

ADVANTAGE - Provides high level of security and ensures data integrity with fast commit processing and fast transaction time by transmitting random session key between the terminal and smartcard.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart illustrating the terminal-smartcard mutual authentication method.

Terminal (102)
Smartcard (104)
pp; 31 DwgNo 1/4

Title Terms: TRANSACTION; AUTHENTICITY; METHOD; TERMINAL; BUS; SYSTEM; TRANSMIT; RANDOM; SESSION; KEY; TERMINAL; AUTHENTICITY; VALID; VALID; TERMINAL
Derwent Class: T05
International Patent Class (Main): G07F-007/10
File Segment: EPI